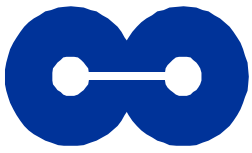
SECURITY BASELINE RECOMMENDATIONS FOR THE SPECIFICATION AND OPERATION OF PUBLIC KEY INFRASTRUCTURE (PKI) COMPONENTS

Prepared for the National Institute of Standards and Technology
Under Contract Number 50SBNB7C1210

May 11, 1998



CYGNACOM SOLUTIONS

Suite 100W♦7927 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

ACKNOWLEDGMENTS

We are grateful to Donna Dodson, Noel Nazario, Bill Burr, and David Cooper for suggestions to improve this document.

INTRODUCTION

1.1 BACKGROUND

A public-key certificate (hereinafter "certificate") binds a public-key value to information that identifies the entity (such as person, organization, account, or site) in control of the corresponding private key (that entity is known as the subject of the certificate or a subscriber). A certificate is used by a "certificate user" or "relying party" that relies upon the accuracy of the binding of the public key to the subject's identity to process data originated by the certificate's subject. The degree to which a certificate user (relying party) can trust the binding embodied in a certificate depends on several factors. These factors include, the practices followed by the certification authority (CA) in authenticating the subscriber; the CA's operating policy, procedures, and security controls; the subscriber's obligations (for example, in protecting the private key); and the stated undertakings and legal obligations of the CA (for example, warranties and limitations on liability).

An X.509 Version 3 certificate may contain a field declaring that one or more specific certificate policies apply to that certificate [1]. According to X.509, a certificate policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." A certificate policy may be used by a certificate user to decide whether a certificate, and the binding therein, is sufficiently trustworthy for a particular application. The certificate policy concept is an outgrowth of the policy statement concept developed for Internet Privacy Enhanced Mail [2] and expanded upon in [3].

A more detailed description of the practices followed by a CA in issuing and otherwise managing certificates may be contained in a certification practice statement (CPS) published by or referenced by the CA. According to the American Bar Association Digital Signature Guidelines (hereinafter "ABA Guidelines"), "a CPS is a statement of the practices which a certification authority employs in issuing certificates." [4]

A Certificate Policy and Certification Practices Statement Framework has been developed to assist the writers of certificate policies and/or certification practices statements [5]. The Framework provides a comprehensive list of topics that potentially, at the CP and CPS writer's discretion, need to be covered in a CP or CPS. At the highest level, the topics to be considered include: Introduction; General Provisions; Identification and Authentication; Operational Requirements; Physical, Procedural, and Personnel Security Controls; Technical Security Controls; Certificate and CRL Profile; and Specification Administration.

1.2 PURPOSE AND SCOPE

The purpose of this document is to provide recommended baseline security requirements for the use and operation of Certification Authorities and other Public Key Infrastructure Components within the Federal Government. These baseline security requirements coincide with most of the topics outlined in the CP and CPS Framework.

The term baseline is used to define the minimum security requirements acceptable for low assurance certificates. The agencies may use more stringent security measures. Relaxing security controls will require tightening security controls in other areas. The relationship among the various security controls and how to perform trade-offs among them is beyond the scope of this document.

This document also provides guidance to Federal Agencies and auditors on how to check the operations of PKI components for compliance with the CP and CPS.

The scope of the document excludes rationale behind the recommendations and trade-offs among various alternatives.

1.3 APPROACH

The approach taken in the document is to expand on the work done in the CP and CPS Framework by providing the following for each element:

- A brief description of the element – This assists in providing an explanation of what the element is.
- Objective for the element – This provides an explanation of why the element is included in the CP and CPS and how it contributes to the trust in the binding between a public key and subscriber.
- Security Criticality – This describes how critical this element is to the security of the PKI.
- Non-Security Criticality – This describes how critical the element is relative to other aspects of the PKI.
- Examples – This provides examples of stipulations for the element.
- Baseline Recommendation – This provides specific recommendations for baseline requirements to be considered by the Federal Agencies for their PKI components. Generally, these recommendations apply to both the CP and CPS. If there are differences in the recommended language, they are explicitly stated.

- Compliance Audit Procedure – This describes how the CA's compliance with the CP and CPS for the element should be checked by the compliance auditor.

1.4 AUDIENCE

This document is targeted at the Federal PKI policy writers, managers, operations personnel, and compliance auditors. The document is intended to provide a detailed guide for those writing or reviewing baseline security requirements CP and CPS documents. Hence, the document assumes some familiarity with PKI, CP and CPS concepts.

1.5 DOCUMENT ORGANIZATION

This section has provided an introduction to the document. Section 2 contains definitions of terms used in the document. Section 3 provides policy guidance, including baseline security requirements for the various elements.

2 DEFINITIONS

Activation data: Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass-phrase, or a manually-held key share).

CA-certificate: A certificate for one CA's public key issued by another CA.

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification path: An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to validate the certificate of the final object in the path.

Certification Practice Statement (CPS): A statement of the practices which a certification authority employs in issuing certificates.

Issuing certification authority (issuing CA): In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Policy mapping: Recognizing that, when a CA in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain.

Policy qualifier: Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Practices and policy specification: A list of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework.

Registration Authority (RA): An entity that is responsible for identification and authentication of certificate subscribers, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying party: A recipient of a certificate who relies on certificates and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Subject certification authority (subject CA): In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (also see Issuing certification authority).

Subscriber: An entity who is the subject of a certificate and is not a CA or RA. The terms “subject” and “subscriber” are used interchangeably in this document.

3 SECURITY RECOMMENDATION

This Baseline Security Recommendation addresses the following components :

1. Introduction
2. General Provisions
3. Identification and Authentication
4. Operational Requirements
5. Physical, Procedural, and Personnel Security Controls
6. Technical Security Controls
7. Certificate and CRL Profile
8. Specification Administration

Components can be further divided into subcomponents, and a subcomponent may comprise multiple elements. The following subsections expand upon the contents of a practices and policy specification, as described in Section 1.3 Approach.

It is not necessary for a certificate policy or a CPS to include a concrete statement for every such topic. Rather, a particular certificate policy or CPS may state "no stipulation" for a component, subcomponent, or element on which the particular certificate policy or CPS imposes no requirements. In this sense, the list of topics can be considered a checklist of topics for consideration by the certificate policy or CPS writer. It is recommended that every component and subcomponent be included in a certificate policy or CPS, even if there is "no

stipulation"; this will indicate to the reader that a conscious decision was made to include or exclude that topic. This avoids inadvertent omission of topics, while facilitating comparison of different certificate policies or CPSs, e.g., when making policy mapping decisions.

3.1 INTRODUCTION

This component identifies and introduces the practices and policy specification, and indicates the types of entities and applications for which the specification is targeted. This component has the following subcomponents:

1. Overview
2. Identification
3. Community and Applicability
4. Contact Details

3.1.1 Overview

Description: This subcomponent provides a general introduction to the specification.

Objective: The objective is to provide an executive summary of the policy and practice statement to the relying party and the reader.

Security Criticality: This subcomponent is not security critical

Non-Security Criticality: Some users may read only the overview, and hence it is critical that a reader can determine from this section whether she should use the policy.

Examples: This policy applies to CAs, RAs, subscribers and relying parties. CPSs in support of this policy may identify specific applications and types of data to be covered. Examples are: general electronic mail, intra-agency official communications, and intra-agency office automation applications (e.g., time and attendance, small purchase requisition, travel order, travel expense vouchers, etc.)

Baseline Recommendation: This policy is recommended for use by the United States Federal Agencies in operation of CAs and RAs. This policy also includes requirements that apply to subscribers, relying parties, and repositories. This policy is suitable to support applications and data critical to the mission of most Government agencies, but those not impacting economic stability or the physical safety of property, groups or individuals.

Compliance Audit Procedure: The auditor shall check that the overview is consistent with the rest of the policy and is complete in terms of applications for which the policy is to be used, the community it serves, and the PKI components to which it applies.

3.1.2 Identification

Description: This subcomponent provides any applicable names or other identifiers, including ASN.1 object identifiers, for the CP and CPS. Object Identifiers have unique names and are registered (see [6] & [7] for additional information) under a hierarchical naming scheme.

Objective: The objective is to provide a common reference name for CP and CPS and to provide object identifiers for CP that can be used in X.509 V3 certificates.

Security Criticality: The object identifier is security critical because its value in X.509 certificates is used in determining the validity of a certificate (trust) path.

Non-Security Criticality: This subcomponent may be critical with respect to legal or contractual concerns. .

Examples: For the common reference names: DoI Basic Assurance Policy (02/03/99), Electronic Mail Policy - version 1.1, Small purchases and obligations policy, etc.

For the object identifier: { 2 16 840 101 3 2 1 5 }.

Baseline Recommendation: Basic Assurance Policy; Object Identifier {2 16 840 101 3 2 1 X}. The CP and CPS can be found at [agency/company URL]. CP Object Identifiers may be obtained from the NIST Computer Security Objects Register (CSOR) at http://csrc.nist.gov/csor.

Compliance Audit Procedure: The auditor shall check that the common reference name is meaningful and descriptive of the CP or CPS. The auditor shall check with the appropriate object registry that the object identifier is registered, that it corresponds to the common reference name, and that the full text of the CP is available for inspection. The auditor shall access the CP and CPS from the defined location and verify that they are accurate and current.

3.1.3 Community and Applicability

This subcomponent contains the following elements:

- Types of entities registered as CAs, RAs, and subscribers

- A list of applications for which the issued certificates are suitable
- A list of applications to which use of the issued certificates is restricted. (This list implicitly prohibits all other uses for the certificates.)
- A list of applications for which use of the issued certificates is prohibited

3.1.3.1 Types of Entities

Description: This element provides a list of types of entities that can act as CA, type of entities that can act as RA, and types of entities that can be subscribers. The CA and RA entities are people in positions of trust. The subscriber entities include people and applications that use the certificates generated by the CAs.

Objective: The objective is to define the scope in terms of who can be a CA, RA, or subscriber.

Security Criticality: This element is security critical to ensure that the CAs and RAs are responsible entities.

Non-Security Criticality: This is critical from operational viewpoint to ensure that the subscribers have easy access to a RA or the CA. It makes the initial subscriber authentication, CA public key certificate revocation notification, and rekey simpler.

Examples: CAs are agency security offices at the headquarters; RAs are local security offices at the agency regional offices, or the badging authority at the agency regional offices; subscribers are the agency employees and on-site contract personnel.

Baseline Recommendation: In order to provide centralized administration and enhance security, operation of the CA should be centralized and coordinated among all the units of an agency. CA services may be provided by the agency or by an external organization vetted for compliance with the applicable policies and regulations. The RA should be operated by the same organization that issues agency badges. Subscribers should generally be limited to agency personnel. An agency that provides services to citizens could also issue certificates to the citizens it serves. The issuance of certificates to contractor personnel should only take place when the length and nature of the contract warrant it. Contractors should be encouraged to make their own arrangements for certificate services.

Compliance Audit Procedure: The auditor shall obtain all the current CA certificates, all the current RA certificates, and a statistical sample of current subscriber certificates. The auditor shall review the subject names in these certificates and initial registration identification and

authentication evidence to verify against the claims of who can be a CA, who can be an RA, and who can be a subscriber.

3.1.3.2 Types of Applications

Description: This element contains up to three lists. The first contains the applications for which the certificate may be used to provide security services. The second list contains the applications the to which use of the certificate is restricted. If this list is present, the other two lists need not be present. If they are present, they are ignored since this list implicitly prohibits all other applications. The third list contains applications for which the certificate may not be used.

Objective: This element identifies the applications and circumstances for which the use of the certificates is allowed and the circumstances and applications for which the use of the certificate is disallowed.

Security Criticality: This element is not security critical.

Non-Security Criticality: This element is critical to the liability that the CA assumes, if the applications the certificate is restricted to are listed. The application restriction is enforced on the relying parties and their certificate processing systems by making the certificate policy field critical and putting the policy in the field.

Examples: List of suitable applications: electronic mail, personnel actions, travel orders, time sheets, etc. List of restricted applications: credit card purchases. List of prohibited applications: classified applications, payroll, electronic transactions and contracts over the value of $2,500.

Baseline Recommendation: The baseline policy should not include a list of restricted applications. The list of suitable applications are: electronic mail, personnel actions, official agency memos, purchase requisitions, personnel actions, travel orders, time and attendance, and travel expense vouchers. The list of prohibited applications should include any classified applications, payroll, and electronic contracts, purchases and fund transfers valued at greater than $2,500.

Compliance Audit Procedure: None

3.1.4 Contact Details

Description: This subcomponent includes the name and mailing address of the authority that is responsible for the registration, maintenance, and interpretation of this certificate policy or

CPS. It also includes the name, electronic mail address, telephone number, and fax number of a contact person.

Objective: The objective of this subcomponent is to provide information on the organization to contact in case further explanation or revision to the policy is desired.

Security Criticality: This component is not security critical.

Non-Security Criticality: This component is critical in providing a point of contact for inquiries, clarifications, and revisions regarding the use of the certificate policy.

Examples: The examples are self-evident.

Baseline Recommendation: The organization should be the agency security policy office. The contact person should be the agency security officer or designee.

Compliance Audit Procedure: The auditor shall check with the contact person to ensure that he and the organization are responsible for the maintenance of the policy and/or CPS. The auditor shall verify that the organization listed in this subcomponent is subordinate to the organization implied by the CP object identifier.

3.2 GENERAL PROVISIONS

This component specifies any applicable presumptions on a range of legal and general practices topics. This component contains the following subcomponents:

1. Liability
2. Obligations
3. Financial Responsibility
4. Interpretation and Enforcement
5. Fee
6. Publication and Repositories
7. Compliance Audit
8. Confidentiality
9. Intellectual Property Rights

The recommendations for this component are beyond the scope of this paper. However, Appendix A contains some preliminary suggestions for this topic.

3.3 IDENTIFICATION AND AUTHENTICATION

This component describes the procedures used to authenticate a certificate applicant to a CA or RA prior to certificate issuance. It also describes how parties requesting rekey or revocation are authenticated. This component also addresses naming practices, including name ownership recognition and name dispute resolution. This component has the following subcomponents:

1. Initial Registration
2. Routine Rekey
3. Rekey After Revocation
4. Revocation Request

3.3.1 Initial Registration

Description: This subcomponent includes the following elements regarding identification and authentication procedures during entity[1] registration or certificate issuance:

1. Types of names assigned to the subject
2. Whether names have to be meaningful or not
3. Rules for interpreting various name forms
4. Whether names have to be unique
5. How name claim disputes are resolved
6. Recognition, authentication, and role of trademarks
7. If and how the subscriber must prove possession of the companion private key for the public key being registered
8. Authentication requirements for organizational identity of subscriber (CA, RA, or end entity)
9. Authentication requirements for a subscriber or the person acting on behalf of a subscriber (e.g., CA, RA, or end entity), including:
   (a) Type and number of pieces of identification required
   (b) Procedure for validating the pieces of identification provided
   (c) If the individual must present himself personally to the authenticating RA or CA
   (d) How is it established that a requesting individual can represent another entity as the subscriber on the certificate.

Objective: The purpose of this subcomponent is to ensure that secure procedures are used to authenticate subscribers of certificates (i.e., subject CAs, subject RAs, and subscribers). The subcomponent also ensures that the names are properly assigned to these entities.

[1] The entities are CAs, RAs, and subscribers.

Security Criticality: This subcomponent is extremely security critical since accurate identification and authentication is the basis for trust in the binding between the subscriber and the subscriber public key.

Non-Security Criticality: This subcomponent is critical to subscriber non-repudiation.

Examples: Examples of types of names are X.500 Distinguished Names (DN), RFC822 names, and X.400 O/R names. Examples of rules for interpreting name forms are given in the corresponding X.500, RFC822, and X.400 standards.

Baseline Recommendation: Use of X.500 DN names is recommended. These names are meaningful and unique when managed properly. These names shall be made completely unique by using middle initial in a common name or adding a sequential suffix at the end of the first name (e.g., employee id, phone number or extension).

Use of obviously inappropriate names or names known to belong to someone else shall not be allowed.

The subscribers are required to provide a proof of possession of the companion private key for the public key being registered as described in the MISPC [8].

The subject CAs, RAs, and other organizational subscribers shall be organizationally authenticated by a signed letter from the agency head on the agency letter head identifying the person responsible for the operation of the entity.

The individual subscribers as well as the individuals representing an organization shall be authenticated using the same procedure as the agency badging procedure. This will require the person to present himself to the CA or a RA.

Compliance Audit Procedure: The auditor shall select all CA and RA initial registration certificates issued since the last audit, and a statistical sample of subscriber initial registration certificates issued since the last audit. The auditor shall obtain the authentication documents for these certificates. The auditor shall ensure that the subject name in each certificate is a valid X.500 DN name for the organization or individual, and that appropriate authentication information was provided for the individual. If the certificate is for the CA or a RA, the auditor shall examine the letter from the agency head for accuracy and completeness.

3.3.2 Routine Rekey

Description: This subcomponent describes the procedure for updating or renewing CA, RA, and end entity certificates. During this process, the existing binding between the certificate subscriber and the public key in a certificate that has recently expired or is about to expire, is extended by issuing a new certificate with a new public key.

Objective: The purpose of this subcomponent is to establish how the integrity of the binding between the subscriber and the public key is maintained as new certificates are issued.

Security Criticality: This subcomponent is extremely security critical since accurate identification and authentication is the basis for trust in the binding between the subscriber and the subscriber public key.

Non-Security Criticality: This subcomponent is critical to subscriber non-repudiation.

Examples: Same as the initial registration; signed rekey request with the current valid private key.

Baseline Recommendation: All entities (subject CAs, RAs, and subscribers) shall be authenticated using the MISPC message Certificate Renewal Request in Section 3.5.2 in [8].

Compliance Audit Procedure: The auditor shall take a statistical sample of rekey (renew) requests since the last audit. The auditor shall verify that the requests were properly signed and that the information in the requests was used to produce the corresponding certificates.

3.3.3 Rekey After Revocation

Description: This subcomponent describes the procedure for updating or renewing CA, RA, and end entity certificates after they have been revoked. This subcomponent shall cover both the revocation due to key compromise and revocation due to reasons other than key compromise.

Objective: The purpose of this subcomponent is to maintain the integrity of binding between the subscriber and the public key as new certificates are issued.

Security Criticality: This subcomponent is extremely security critical since accurate identification and authentication is the basis for trust in the binding between the subscriber and the subscriber public key.

Non-Security Criticality: This subcomponent is critical to subscriber non-repudiation.

Examples: Same as the initial registration.

Baseline Recommendation: If the revocation is due to key compromise, the process shall be the same as the initial registration. If the revocation is due to reasons where the holding of the private key is not in question (e.g., change in name or privileges), the process shall be the same as the routine rekey. If the revocation is due to reasons where the holding of private key can not be guaranteed, the process shall be the same as the initial registration.

Compliance Audit Procedure: The auditor shall verify that the CA treats rekey after revocation in accordance with the stated requirements .

3.3.4 Revocation Request

Description: This subcomponent describes the identification and authentication procedures for a revocation request by each subscriber type (CA, RA, and end entity).

Objective: The purpose of this subcomponent is to ensure that a certificate is only revoked at the request of a bona-fide entity, i.e., CA, RA or the subscriber.

Security Criticality: This element is not security critical.

Non-Security Criticality: This element is critical for user's ability to continue to conduct business and others not causing denial-of-service.

Examples: Signed request by the subscriber, signed request by the RA, personal appearance by the subscriber at the CA.

Baseline Recommendation: The CA shall revoke a subscriber certificate if a MISPC compliant signed transaction is received from the subscriber. The CA shall also revoke a subscriber certificate if a signed request is received from an authorized RA. The subscribers shall be able to visit the local RA and show their agency badges to request revocation.

Compliance Audit Procedure: The auditor shall take a statistical sample of revocation requests since the last audit. The auditor shall verify that the requests were properly signed and that the information in the requests was used to revoke the corresponding certificates.

3.4 OPERATIONAL REQUIREMENTS

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, or end entities with respect to various operational activities. This component consists of the following subcomponents:

1. Certificate Application
2. Certificate Issuance
3. Certificate Acceptance
4. Certificate Suspension and Revocation
5. Security Audit Procedures
6. Records Archival
7. Key Changeover
8. Compromise and Disaster Recovery
9. CA Termination

Within each subcomponent, separate consideration may be given to issuing CAs, repositories, subject CAs, RAs, and end entities.

3.4.1 Certificate Application

Description: This subcomponent is used to state requirements regarding subscriber enrollment and request for certificate issuance.

Objective: To allow subscribers the ability to apply for a certificate.

Security Criticality: This subcomponent must provide a reliable request that can be validated by the RA (or CA).

Non-Security Criticality: This subcomponent is not otherwise critical.

Examples: In a low assurance environment, a user generates his or her key pair locally. The public key is packaged in a certificate generation request from the RA to the CA or from the subscriber to the CA.

Baseline Recommendation: The CA shall generate certificates upon receiving requests from authorized RAs and subscribers. These certificate generation requests shall conform to the MISPC transactions for certificate generation.

Compliance Audit Procedure: The auditor shall take a statistical sample of the certificate generation requests since the last compliance audit, and review the CA audit information to ascertain that these certificate requests were properly processed by the CA.

3.4.2 Certificate Issuance

Description: This subcomponent is used to state requirements regarding issuance of a certificate and notification to the applicant of such issuance.

Objective: To validate a certificate request and if valid, generate a certificate.

Security Criticality: To reliably validate certificate requests and to generate a signature during certificate generation is critical.

Non-Security Criticality: This subcomponent is not otherwise critical.

Examples: The CA receives a request from the RA requesting a certificate using the request supplied information. The CA verifies the RA signature and based on successful verification, generates a certificate. A copy of the certificate is returned to the RA and another is sent to the repository.

Baseline Recommendation: The CA shall produce a certificate upon receiving a properly formatted and signed request from the RA or subscriber as specified in the MISPC. The CA shall send the newly created certificate to the repository.

Compliance Audit Procedure: The auditor shall take a statistical sample of the certificate generation requests since the last compliance audit and review the CA audit information and repository audit information to ascertain that these certificates were properly issued and were sent to the repoistory in a timely manner.

3.4.3 Certificate Acceptance

Description: This subcomponent is used to state requirements for the acceptance of an issued certificate by the subscriber and consequent certificate publication.

Objective: To be able to receive a certificate following a valid certificate request.

Security Criticality: It is important that the subscriber be able to validate the issued certificate.

Non-Security Criticality: It is critical that the certificates issued are correct and based on a valid requests.

Examples: Following a request for a certificate, a user receives a returned certificate. The user then validates the certificate.

Baseline Recommendation: Upon receipt, the subscriber may optionally validate the certificate.

Compliance Audit Procedure: None.

3.4.4 Certificate Suspension and Revocation

Description: This subcomponent addresses the following elements:

- Circumstances under which a certificate may be revoked
- Who can request the revocation of the entity certificate
- Procedures used for certificate revocation requests
- Revocation request grace period available to the subscriber
- Circumstances under which a certificate may be suspended
- Who can request the suspension of a certificate
- Procedures to request certificate suspension
- How long the suspension may last
- If a CRL mechanism is used, the issuance frequency
- Requirements on relying parties to check CRLs
- On-line revocation/status checking availability
- Requirements on relying parties to perform on-line revocation/status checks
- Other forms of revocation advertisements available
- Requirements on relying parties to check other forms of revocation advertisements
- Any variations on the above stipulations when the suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation).

Objective: The objective of this subcomponent is to inform the subscribers and the relying parties of the revocation and suspension policy.

Security Criticality: This subcomponent is security critical since it ensures that the relying parties revocation checking requirements are aligned with the CA revocation and revocation notification policy. Furthermore, the relying parties must perform the revocation checks according to this subcomponent in order to trust the certificate.

Non-Security Criticality: It is not critical otherwise.

Examples: Examples for the various elements of this component are:

- **Circumstances under which a certificate may be revoked:** employee termination and employee name change due to change in marital status.
- **Who can request the revocation of the entity certificate:** entity, RA
- **Procedures used for certificate revocation request:** electronic signed message from the subscriber or the RA
- **Revocation request grace period available to the subscriber:** 7 days
- **Circumstances under which a certificate may be suspended:** subscriber reporting a misplaced token, RA suspecting potential compromise while subscriber is not accessible (e.g., on vacation).
- **Who can request the suspension of a certificate:** subscriber, RA
- **Procedures to request certificate suspension:** digitally signed request from RA
- **How long the suspension may last:** 30 days
- **If a CRL mechanism is used, the issuance frequency:** weekly
- **Requirements on relying parties to check CRLs:** always check the latest CRL
- **On-line revocation/status checking availability:** yes
- **Requirements on relying parties to perform on-line revocation/status checks:** must check for financial transactions
- **Other forms of revocation advertisements available:** web URL
- **Requirements on relying parties to check other forms of revocation advertisements:** must check the web URL
- **Any variations on the above stipulations when the suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation):** the revocations are pushed to the subscribers

[there should be consistency among the bulleted lists]

Baseline Recommendation: The following are the recommendations for the various elements of this subcomponent:

- **Circumstances under which a certificate may be revoked:** subscriber affiliation termination, subscriber name change, DN change due to reorganization, subscriber key compromise, subscriber token loss.
- **Who can request the revocation of the entity certificate:** subscriber, RA
- **Procedures used for certificate revocation request:** digitally signed request from the subscriber or the RA in accordance with MISPC revocation request
- **Revocation request grace period available to the subscriber:** 1 day

- **Circumstances under which a certificate may be suspended:** subscriber reporting misplaced token, suspected activity while subscriber is not available
- **Who can request the suspension of a certificate:** subscriber, RA
- **Procedures to request certificate suspension:** same as revocation
- **How long the suspension may last:** 30 days
- **If a CRL mechanism is used, the issuance frequency:** weekly
- **Requirements on relying parties to check CRLs:** always check the latest CRL
- **On-line revocation/status checking availability:** None
- **Requirements on relying parties to perform on-line revocation/status checks:** None
- **Other forms of revocation advertisements available:** None
- **Requirements on relying parties to check other forms of revocation advertisements:** None
- **Any variations on the above stipulations when the suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation):** None

Compliance Audit Procedure: The auditor shall review a statistical sample of certificate revocation and suspension requests since the last compliance audit to ensure that the CRL generation and distribution is according to the policy.

3.4.5 Security Audit Procedures

Description: This subcomponent is used to describe event logging and audit systems, implemented for the purpose of maintaining a secure environment. Please note that the term auditor in this section means audit log reviewer and not the compliance auditor. Elements include the following:

- Types of events recorded
- Frequency with which audit logs are processed or audited
- Period for which audit logs are kept
- Protection of audit logs
  - Who can view audit logs
  - Who can modify the audit logs
  - Who can delete the audit logs
- Audit log back up procedures
- Whether the audit log accumulation system is internal or external to the entity
- Whether the subscriber who caused an audit event to occur is notified of the audit action
- Vulnerability assessments

Objective: To provide the mechanism by which someone can review security relevant events to reconstruct what occurred.

Security Criticality: This subcomponent is critical to ensure that the security relevant events are reviewable in order to verify secure operation of the CA.

Non-Security Criticality: This subcomponent is otherwise critical for compliance audit and dispute resolution.

Examples: The following are the examples for the various elements of this component

- **Types of events recorded:** certificate generation request, certificate generation, CA key changeover
- **Frequency with which audit logs are processed or audited:** monthly audit logs are archived
- **Period for which audit logs are kept:** 1 month, after which they become part of the archived records
- **Protection of audit logs**
  - Who can view audit logs: auditor
  - Who can modify the audit logs: no one may modify
  - Who can delete the audit logs: only auditor may delete after archiving
- **Audit log back up procedures:** auditor saves the log to archival medium
- **Whether the audit log accumulation system is internal or external to the entity:** internal
- **Whether the subscriber who caused an audit event to occur is notified of the audit action:** no
- **Vulnerability assessments:** weekly review of audit log for potential security breaches

Baseline Recommendation: The audit period should be specified in the policy.

- **Types of events recorded:** certificate generation requests, revocation requests, certificate creation, CRL generation, certificate and CRL issuance, CA key change, CA software change, and CA administrator activities, including audit and archive management.
- **Frequency with which audit logs are processed or audited:** audit logs are reviewed weekly and archived monthly
- **Period for which audit logs are kept:** for one month, after which they become part of archived records

- **Protection of audit logs**: For CPS, the protection is achieved by using an audit subsystem that is designed, implemented, and operated to meet the C2[2] audit requirements.
  - **Who can view audit logs:** only auditor may view them.
  - **Who can modify the audit logs**: no one may modify
  - **Who can delete the audit logs:** auditor may delete after archiving
- **Audit log back up procedures:** system dependent. The agency may describe the procedures for its CA.
- **Whether the audit log accumulation system is internal or external to the entity:** The audit information shall be internal to the CA.
- **Whether the subscriber who caused an audit event to occur is notified of the audit action:** The subscribers need not be notified
- **Vulnerability assessments:** The auditor will review audit logs weekly and in case of reported or suspected compromise. The compliance auditor requirements are addressed under the compliance audit subcomponent.

Compliance Audit Procedure: The compliance auditor will review the audit log to verify that certificate generation and revocation requests are being audited. The compliance auditor shall obtain a list of all CA key changeovers since the last audit and verify that each event was audited. The compliance auditor shall verify the protection on the audit log.

3.4.6 Records Archival

Description: This subcomponent is used to describe general records archival (or records retention) policies, including the following:

- Types of events recorded
- Retention period for archive
- Protection of archive
  - Who can view the archive
  - Who can modify the archive
  - Who can delete the archive
- Archive backup procedures
- Requirements for time-stamping of records
- Whether the archive collection system is internal or external
- Procedures to obtain and verify archive information

[2] C2 is a level of security protection defined in the "Orange Book". For further information on C2, see the Trusted Computer System Evaluation Criteria [21].

- If a non-repudiation of data service is dependent on keys provided by the CA, the service should ensure that all relevant keys of the CA (revoked or expired) and the time stamped revocation lists are archived and certified by a current authority

Objective: To maintain a reliable archive of records in order to resolve disputes and investigate potential security breaches.

Security Criticality: It is critical that records be available for investigating security breaches

Non-Security Criticality: This subcomponent is otherwise critical for dispute resolution.

Examples: The following are examples for the various elements of this subcomponent:

- **Types of events recorded:** certificate generation requests, certificate generation, CA key changeover
- **Retention period for archive:** 30 years
- **Protection of archive**
  - Who can view the archive: compliance auditor, CA administrator
  - Who can modify the archive: no one
  – Who can delete the archive: no one.
- **Archive backup procedures:** Two different copies of the archive are stored under the control of two different persons, at two different locations. When the archive is accessed, the two copies shall be compared to verify that the archives have not been modified.
- **Requirements for time-stamping of records:** signed by a time stamp service
- **Whether the archive collection system is internal or external:** internal
- **Procedures to obtain and verify archive information:** clean room

Baseline Recommendation: The following are baseline recommendations for the various elements of this subcomponent:

- **Types of events recorded:** audit log. Since audit log contains the events to be archived, they are available from audit log.
- **Retention period for archive:** 30 years
- **Protection of archive**
  - Who can view the archive: compliance auditor, CA administration
  - Who can modify the archive: No one may modify the archive. The CPS shall also state that this requirement is met by technical or procedural controls.
  - Who can delete the archive: No one may delete the archive. The CPS shall also state that this requirement is met by technical or procedural controls.

- **Archive backup procedures:** Two copies of the archive shall be made. These copies shall be stored in separate physically secure locations under the control of two different individuals.
- **Requirements for time-stamping of records:** None
- **Whether the archive collection system is internal or external:** Internal
- **Procedures to obtain and verify archive information:** In order to verify the information, a physically secure, stand-alone system, known to work correctly shall be used. Two archives shall be compared prior to using the archive information.

Compliance Audit Procedure: The compliance auditor shall spot check the archive to ensure that audit logs are being archived. The compliance auditor shall verify the protection on the archive, especially the physical security of both the archival storage sites. The compliance auditor shall also validate that the two copies are under the control of two different persons.

3.4.7 Key Changeover

Description: This subcomponent describes the procedures to provide a new CA public key to subscribers. This may be the key of the CA that issues certificates directly to the subscribers, or the key of a "root" CA, that certifies other CAs but not subscribers. In either case, it is the key of the trusted CA from which all other keys are validated.

Objective: The objective of this requirement is to ensure that the subscribers continue to maintain a chain of trust within the CA and potentially global PKI context.

Security Criticality: It is critical that the subscribers continue to maintain a chain of trust.

Non-Security Criticality: This subcomponent is otherwise not critical.

Examples: The CA key is provided using physical hand-off to the RA. The RA in turn provides the key to the users.

The new CA key is put in a self-signed public key certificate. The whole certificate is countersigned using the old (current) CA private key.

The self-signed CA certificate contains the hash of the new keying material. Thus, subscribers upon receiving a new self-signed CA certificate can validate the key against the hash information from the previous certificate.

Baseline Recommendation: The CA certificate shall be self-signed. It shall contain the hash of the next keying material (in the case of DSS, public key and public key parameters shall be hashed).

Compliance Audit Procedure: The auditor shall examine all CA certificates issued since the last audit and verify that they are accurate, including the hash of the next keying material.

3.4.8 Compromise and Disaster Recovery

Description: This subcomponent describes requirements for compromise or disaster notification and recovery procedures. Each of the following circumstances may need to be addressed separately:

- The recovery procedures used if computing resources, software, and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is reestablished, which certificates are revoked, whether the entity key is revoked, how the new entity public key is provided to the users, and how the subscribers are re-certified.
- The recovery procedures used if the entity public key is revoked. These procedures describe how a secure environment is reestablished, how the new entity public key is provided to the users, and how the subscribers are re-certified.
- The recovery procedures used if the entity key is compromised. These procedures describe how a secure environment is reestablished, how the new entity public key is provided to the users, and how the subscribers are re-certified.

Objective: To ensure recovery and continuity of operations following disasters or key compromises.

Security Criticality: It is critical that the secure environment be reestablished after compromise.

Non-Security Criticality: It is critical that the CA continues to operate in order to provide service to subscribers and relying parties.

Examples: The examples are self-evident from the recommendations below.

Baseline Recommendation: The following are the recommendations for the various elements of this subcomponent:

- **Recovery Procedures:** The CA will reestablish a secure environment. A new CA key pair will be generated. All certificates will be revoked. The new key will be physically provided to the RAs. The RAs shall report the CA key revocation to all subscribers and provide them with the new CA key. The RAs will request new certificates for themselves

and for subscribers. The RAs and subscribers need not generate new key pairs. They just need to request new certificates.

- **CA Key Revocation:** In the case of CA key revocation, the same procedures as the recovery procedures described above shall be followed.
- **CA Key Compromise:** In the case of CA key compromise, the same procedures as the recovery procedures described above shall be followed.

Compliance Audit Procedure: The auditor shall examine if there has been any need for recovery procedures to be followed since the last compliance audit. If so, the auditor shall verify that the procedures were followed.

3.4.9 CA Termination

Description: This subcomponent describes requirements relating to procedures for termination and for termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records.

Objective: To provide the policy procedure for changing a CA or RA.

Security Criticality: This subcomponent is not security critical.
‘

Non-Security Criticality: This subcomponent is otherwise critical to ensure that proper information is made available in the future for dispute resolution.

Examples: The CA archive records are sent to another CA or a trusted party.

Baseline Recommendation: Upon CA or RA termination, the agency security office shall take possession of all CA or RA archive records.

Compliance Audit Procedure: None.

3.5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This component describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to perform securely the functions of key generation, subscriber authentication, certificate issuance, certificate revocation, audit, and archiving.

This component can also be used to define non-technical security controls on repositories, subject CAs, RAs, and end entities. The non-technical security controls for the subject CAs, RAs, and end entities could be the same, similar, or very different.

These non-technical security controls are critical to trusting the certificates since lack of security may compromise CA operations resulting, for example, in the creation of certificates or CRLs with erroneous information or the compromise of the CA private key.

This component consists of three subcomponents:

- Physical Security Controls
- Procedural Controls
- Personnel Security Controls

Within each subcomponent, separate consideration will, in general, need to be given to each entity type, that is, issuing CA, repositories, subject CAs, RAs, and end entities.

Security controls normally reflect the organizational security policy (for additional information on security policy, see [9]).

3.5.1 Physical Security Controls

Description: In this subcomponent, the physical controls on the facility housing the entity systems are described. Topics addressed may include:

- Site location and construction
- Physical access
- Power and air conditioning
- Water exposures
- Fire prevention and protection
- Media storage
- Waste disposal
- Off-site backup

Objective: Physical security policy indicates the level of protective measures afforded the CA and RA.

Security Criticality: It is critical that the CA and RA resources are not readily available to unauthorized persons. The integrity of the CA and RA is critical.

Non-Security Criticality: There may be a denial of service problem should physical security not be adequate.

Examples: The CA is located in a locked computer room within a secure facility. The facility is either locked or has a guard.

The RA is located in a secure facility. The facility is either locked or has guard.

Baseline Recommendation: The following are the recommendations for the various elements of this component:

- **Site location and construction:** No stipulation.
- **Physical access:** The CA and RA shall be in a secure facility which has locks or guards. Furthermore, the CA shall be in computer room which can be accessed only by authorized CA operators and administrators.
- **Power and air conditioning:** Normal office environment.
- **Water exposures:** Normal office environment.
- **Fire prevention and protection:** Normal office environment.
- **Media storage:** Normal office environment.
- **Waste disposal:** Normal office environment.
- **Off-site backup:** Copies of CA and RA audit and archival data, subscriber I&A evidence, and software shall be kept in a physically secure off-site facility.

Compliance Audit Procedure: The auditor shall inspect the CA and RA facilities to verify the physical security controls.

3.5.2 Procedural Controls

Description: In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.

For each task identified for each role, it should be stated how many individuals are required to perform the task (m of n rules). Identification and authentication requirements for each role may also be defined.

Objective: To provide security controls over sensitive CA functions.

Security Criticality: It is critical that the procedural controls provide adequate protection for the CA.

Non-Security Criticality: Weak procedural controls could lead to a denial of service thereby impacting non-security areas.

Examples: The CA of Bank X uses a dual control split knowledge control. Two of four authorized users must present their token to the CA as an enabling condition.

Baseline Recommendation: The CA shall have the following roles: CA administrator, auditor, archivist, and security officer. The CA computer system shall require individual identification and authentication for each role. The mechanism shall be designed, implemented, and operated to meet the C2 identification and authentication requirement. Each role shall be assigned to a separate individual. The auditor shall be responsible for managing the audit log and archive. The security officer shall be in possession of the CA cryptographic module and shall be responsible for activating and deactivating the module. The CA administrator shall perform all other CA operations related functions. In order for the CA to issue certificates and CRLs, both CA administrator and security officer are required. The administrator is required to bring up the computer system and the security officer is required to activate the cryptographic module. The backed up CA private key shall be under the control of the CA administrator and the security officer. The two copies of the archival records shall be under the control of the auditor and the archivist.

Compliance Audit Procedure: The auditor shall interview the four individuals to verify that they understand and follow their roles and responsibilities.

3.5.3 Personnel Security Controls

Description: This subcomponent addresses the following:

- Background checks and clearance procedures required for the personnel filling the trusted roles
- Background checks and clearance procedures required for other personnel, including janitorial staff
- Training requirements and training procedures for each role
- Any retraining period and retraining procedures for each role
- Frequency and sequence for job rotation among various roles
- Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems
- Controls on contracting personnel, including
  - Bonding requirements on contract personnel
  - Contractual requirements including indemnification for damages due to the actions of the contractor personnel
  - Auditing and monitoring of contractor personnel
  - Other controls on contracting personnel
- Documentation to be supplied to personnel

Objective: To ensure that high integrity personnel are operating the CA.

Security Criticality: Trustworthy personnel are critical to security of a CA.

Non-Security Criticality: This element is otherwise not critical.

Examples: The CA at a large company, checks on the person's references and performs a credit check. Background investigations and security clearance procedures are used to ascertain the trustworthiness of the personnel.

Baseline Recommendation: The following are the recommendations for the various elements of this subcomponent:

- **Background checks and clearance procedures required for the personnel filling the trusted roles:** The procedures shall be the same as the agency secret clearance.
- **Background checks and clearance procedure requirements for other personnel, including janitorial staff:** There are no additional requirements over and beyond what the agency normally does.
- **Training requirements and training procedures for each role:** The personnel shall be trained in their job duties.
- **Any retraining period and retraining procedures for each role:** There are no requirements in this area since the operations are relatively simple.
- **Frequency and sequence for job rotation among various roles:** There are no requirements in this area.
- **Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems:** The agency shall consult its legal counsel and personnel office for specifying disciplinary actions.
- **Controls on contracting personnel, including**
  - Bonding requirements on contract personnel: None
  - Contractual requirements including indemnification for damages due to the actions of the contractor personnel: None
  - Audit and monitoring of contractor personnel: There are no additional requirements over and above what the agency normally does for other matters
  - Other controls on contracting personnel: None
- **Documentation to be supplied to personnel:** The personnel shall be provided appropriate user manuals.

Compliance Audit Procedure: The auditor shall verify that all personnel hired for the CA operations since the last audit meet the requirements of this policy.

3.6 TECHNICAL SECURITY CONTROLS

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). This component may also be used to impose constraints on repositories, subject CAs, and end entities to protect their cryptographic keys and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, audit, and archiving. Technical controls include life-cycle security controls (including software development environment security and trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on repositories, subject CAs, RAs, and end entities.

This component has the following subcomponents:

- Key Pair Generation and Installation
- Private Key Protection
- Other Aspects of Key Pair Management
- Activation Data
- Computer Security Controls
- Life-Cycle Security Controls
- Network Security Controls
- Cryptographic Module Engineering Controls

3.6.1 Key Pair Generation and Installation

Description: Key pair generation and installation need to be considered for the issuing CA, repositories, subject CAs, RAs, and subject end entities. For each of these types of entities, the following questions potentially need to be answered:

1. Who generates the entity public-private key pair?
2. How is the private key provided securely to the entity?
3. How is the entity's public key provided securely to the certificate issuer?

4. If the entity is a CA (issuing or subject) how is the entity's public key provided securely to the users?
5. What are the key sizes?
6. Who generates the public key parameters?
7. Is the quality of the parameters checked during key generation?
8. Is the key generation performed in hardware or software?
9. For what purposes may the key be used, or for what purposes should usage of the key be restricted (for X.509 certificates, these purposes should map to the key usage flags in the X.509 Version 3 certificates)?

Key pairs may be generated by one of the following methods:

1. The subscriber generates his or her keys locally.
2. A trusted third party generates the keys.
3. The CA generates the keys.

Objective: To define the policy on key generation.

Security Criticality: If weak keys are generated, all security is in jeopardy.

Non-Security Criticality: This element is not critical otherwise.

Examples: The subscribers at company X generate DSA key pairs using a FIPS 140-1 [11] level 2 cryptographic module. The private key is confined to the cryptographic module and the public key is sent to the RA.

Baseline Recommendation: The following are the recommendations for the various elements of this subcomponent:

1. **Who generates the entity public, private key pair?** The CAs, RAs, and end entities all generate their own key pairs. Each entity generating its own key pair gives greater confidence that no one else has access to the private; further enhancing non-repudiation of digital signatures.
2. **How is the private key provided securely to the entity?** Since every entity generates its own key pairs, this requirement is not applicable.
3. **How is the entity's public key provided securely to the certificate issuer?** The public key is provided to the CA using signed requests as indicated in the MISPC [8]. The main purpose of issuing a certificate is to bind an entity and its public key accurately. If the correct public key is not provided, the certificate will be useless. If someone can substitute the entity’s public key, the one substituting can act as the entity. Thus, it is

critical that the CA obtains the correct public key. When the CA gets a public key in a transaction digitally signed by an ORA or the subscriber itself, the CA can be sure that the public key is correct.

4. **If the entity is a CA (issuing or subject) how is the entity's public key provided securely to the users?** The keys are provided by the RA using trusted means, such as physical hand-off. In performing encryption or digital signature verification, an entity must have a CA public key that it trusts. In order to ensure the security of digital signatures, the certificate chain must begin with a certificate signed by this CA using the private key corresponding to this trusted public key.
5. **What are the key sizes?** All DSA keys use a 1024 bit modulus, the largest size specified in FIPS 186, the Digital Signature Standard.
6. **Who generates the public key parameters?** The CA generates the parameters. The quality of parameters is important to the security of digital signatures. The CA generation of the parameters using a FIPS compliant system ensures this.
7. **Is the quality of the parameters checked during key generation?** The CA generates the parameters in accordance with the standard. Thus, quality is checked implicitly.
8. **Is the key generation performed in hardware or software?** The CA key is generated in a hardware cryptographic module. Other components (RAs, end entities) may use either a software cryptographic module or a hardware cryptographic module. The generation of a private key in hardware minimizes its chances of being intentionally or accidentally exposed.
9. **For what purposes may the key be used, or for what purposes should usage of the key be restricted?** The keys may be used for digital signature. Note that for X.509 certificates, these purposes should map to the key usage flags in the X.509 Version 3 certificates.

Compliance Audit Procedure: Some of the information here is implicitly verified by verifying the cryptographic module requirement stated later. The auditor shall verify all the CA certificates and a statistical sample of CA issued certificates to validate that the keys are based on 1024 bit modulus.

3.6.2 Private Key Protection

Description: Requirements for private key protection need to be considered for the issuing CA, repositories, subject CAs, RAs, and subject end entities. For each of these types of entity, the following questions potentially need to be answered:

1. What standards, if any, are required for the module used to generate the keys? For example, are the keys certified by the infrastructure required to be generated using US FIPS 140-1 validated cryptographic modules ? If so, what is the required FIPS 140-1 level of the module?

2. Is the private key under n out of m multi-person control? If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?
3. Is the private key escrowed? If so, who is the escrow agent, in what form is the key escrowed (examples include plaintext, encrypted, split key), and what are the security controls on the escrow system?
4. Is the private key backed up? If so, who is the backup agent, in what form is the key backed up (examples include plaintext, encrypted, split key), and what are the security controls on the backup system?
5. Is the private key archived? If so, who is the archival agent, in what form is the key archived (examples include plaintext, encrypted, split key), and what are the security controls on the archival system?
6. Who enters the private key into the cryptographic module? In what form (i.e., plaintext, encrypted, or split key)? How is the private key stored in the module (i.e., plaintext, encrypted, or split key)?
7. Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period?
8. Who can deactivate the private key and how? Examples of how might include: logout, power off, remove token/key, automatic, or time expiration.
9. Who can destroy the private key and how? Examples of how might include token surrender, token destruction, or key overwrite.

Objective: To ensure only the certificate's subject uses the private key.

Security Criticality: Private key protection is a critical security concern. Loss or compromise of the private key jeopardizes the subject's security.

Non-Security Criticality: Loss of the CA private key may result in denial of service.

Examples: The CA uses a FIPS Pub 140-1 validated level 2 cryptographic module.

Baseline Recommendation: The following are the recommendations for the various elements:

1. **What standards, if any, are required for the module used to generate the keys? For example, are the keys certified by the infrastructure required to be generated using modules compliant with the US FIPS 140-1? If so, what is the required FIPS 140-1 level of the module?** The CA keys shall be generated in a FIPS 140-1 level 2 validated

module. The other entity (RA, subscriber) keys shall be generated in a FIPS 140-1 level 1 validated module. Using FIPS 140-1 compliant cryptographic modules helps ensure that the keys generated are sound, and are properly protected. The CA is required to use a higher level of assurance (Level 2) since its trust is more critical.

2. **Is the private key under n out of m multi-person control? If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?** None of the private keys (i.e., CA, RA, or subscribers) need to be under multi-person control, except for the backed up CA private key as described later.
3. **Is the private key escrowed? If so, who is the escrow agent, in what form is the key escrowed (examples include plaintext, encrypted, split key), and what are the security controls on the escrow system?** Since these are digital signature keys, the private keys are not escrowed. Ensuring that a third party or parties does not have access to the private key strengthens signer non-repudiation.
4. **Is the private key backed up? If so, who is the backup agent, in what form is the key backed up (examples include plaintext, encrypted, split key), and what are the security controls on the backup system?** Only the CA is required to back up its private key. The CA private key is backed up so that in case of primary module failure a backup module can be used. If the key were not backed up, the CA would have to rekey and use an out-of-band means to provide the new public key since the old (current) private key would not be available to sign the new public key for in-band rekeying. The backed up private key shall be stored so that it is secure and under split control.[3]
5. **Is the private key archived? If so, who is the archival agent, in what form is the key archived (examples include plaintext, encrypted, split key), and what are the security controls on the archival system?** The private keys are not archived. There is no need to archive signing private keys for verification of digital signatures in the future. Private signature keys must be destroyed immediately after they are no longer in use (e.g., after a private key expires or after rekey).
6. **Who enters the private key into the cryptographic module? In what form (i.e., plaintext, encrypted, or split key)? How is the private key stored in the module (i.e., plaintext, encrypted, or split key)?** This requirement is not applicable since the private key is never entered, except for entering the backed up CA private key. In the case of CA

[3] The following are some of the acceptable alternatives. Under one alternative, the private key is backed up in encrypted form. One person knows the decryption password and another person stores the encrypted private key in a locked cabinet in a physically secure facility. The first person does not have access to the locked cabinet. Under another alternative, the private key is output in split key form. Two different persons store the splits in different locked cabinets. The individuals do not have access to each other's cabinet. Under yet another alternative, the private key is output in plaintext form and stored in a safe which is under two person control.

cryptographic module failure, the backed up private key is entered in a new operational module in the same form (plaintext, encrypted, or split) as it was output for backup.

7. **Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period** A password must be entered by the key owner to activate the private key. The private key must be stored in encrypted form. Storing the private key in encrypted form further protects against misuse of the key by unauthorized individuals. It also provides a degree of protection after successful physical tampering of the cryptographic module. [Isn't the requirement to encrypt the key only when it is exported from the CM?]
8. **Who can deactivate the private key and how? Examples of how might include: logout, power off, remove token/key, automatic, or time expiration.** The owner can deactivate the private key by logging out. It is important that the private key not be usable by unauthorized individuals.
9. **Who can destroy the private key and how? Examples might include token surrender, token destruction, or key overwrite.** The owner may destroy the private key by using the FIPS 140-1 compliant key destruction capability of the module. The private keys must be destroyed immediately after they are no longer in use (e.g., after a private key expires or after rekey).

Compliance Audit Procedure: The auditor shall verify this requirement implicitly by verifying the cryptographic module engineering requirement described later.

3.6.3 Other Aspects of Key Pair Management

Description: Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs, and subject end entities. For each of these types of entity, the following questions potentially need to be answered:

1. Is the public key archived? If so, who is the archival agent and what are the security controls on the archival system? The archival system should provide integrity controls other than digital signatures since: the archival period may be greater than the cryptanalysis period for the key (i.e., temporal exposure of the key to exhaustive attack) and the archive requires tamper protection, which is not provided by digital signatures.
2. What are the usage periods, or active lifetimes, for the public and the private key respectively?

Objective: To ensure the private key is not overused and transactions can be verified after the key expires.

Security Criticality: The key change over is critical to reduce the cryptanalysis threat.

Non-Security Criticality: This requirement may be critical to dispute resolution.

Examples: The private key is used for 2 years for signing. The companion public key may be used for signature verification for up to seven years.

Baseline Recommendation: The following are the recommendations for the various elements of this subcomponent:

1. **Public key archival:** The public key is archived. Please see the archival subcomponent for further details. Public key archiving is required to validate digital signatures after a certificate has expired.
2. **What are the usage periods, or active lifetimes, for the public and the private key respectively?** The private key is valid for 3 years for signature. The public key certificate is valid for 3 years and 2 months. For digital signature applications, the public key should be valid for a period of time (this period is dependent on the application) after the private key is no longer used to generate digital signatures, since the verifier will verify a signature some time after the signer has signed. The periods selected are suggestions. They may be changed as long as the cryptanalysis threat and potential CRL size are accounted for. Too long a validity period for a public key increases the chances of the private key compromise due to cryptanalysis. It also increases the sizes of CRLs since an entry must remain on the CRL until after the public key validity period expires.

Compliance Audit Procedure: The auditor shall take a statistical sample of all certificates issued, and examine all CA self-certificates in order to ensure that the validity period for a certificate was no greater than the validity period allowed by the policy.

3.6.4 Activation Data

Description: Activation data refers to data values other than keys that are required to operate cryptographic modules and that need to be protected. Passwords are an example of activation data. Protection of activation data potentially needs to be considered for the issuing CA, subject CAs, RAs, and end entities. Such consideration potentially needs to address the entire life cycle of the activation data from generation through archiving and destruction. For each of the entity types (issuing CA, repository, subject CA, RA, and end entity) all of the questions listed in 3.6.1 through 3.6.3 potentially need to be answered with respect to activation data as well as with respect to keys.

Objective: To ensure the security of activation data required to operate the cryptographic module.

Security Criticality: The password or PIN (i.e., personal identification number) required to activate the cryptographic module is critical to security. If the PIN (or password) is compromised, unauthorized access to the cryptographic module may be possible.

Non-Security Criticality: A lost password could result in denial of service.

Examples: The passwords are generated by the entities themselves. The passwords shall comply with the FIPS guidelines.

Baseline Recommendation: The CAs, RAs, and end entities, shall all generate, change, and manage their passwords in compliance with the password management FIPS [12]. Strong password management is fundamental to secure operations.

Compliance Audit Procedure: The auditor shall interview all CA and RA personnel to verify that they understand the password management requirements and follow them.

3.6.5 Computer Security Controls

Description: This subcomponent is used to describe computer security controls such as: use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object reuse, audit, identification and authentication, trusted path, security testing, and penetration testing. Product assurance may also be addressed.

A computer security rating for computer systems may be required. The rating could be based, for example, on the Trusted Computer System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC)," or the Common Criteria. This subcomponent can also address requirements for product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activities undertaken.

Objective: To define computer security features.

Security Criticality: The security features of the computer are critical to maintain the security and integrity of CA and RA.

Non-Security Criticality: This component is not critical otherwise.

Examples: The CA shall use an operating system that is designed, implemented, and operated to meet the C2 security requirements.

Baseline Recommendation: The CA shall use an operating system that is designed, implemented, and operated to meet the C2 security requirements. Using a C2 operating system will ensure that the CA is operating securely and its audit log is accurate.

Compliance Audit Procedure: The auditor shall verify that the operating system is configured and operated with C2 security features. The C2 determination can be based on a NIST and NSA approved C2 evaluation, agency analysis, vendor claims, and a combination of the above. Whether the operating system is evaluated or not, the auditor shall verify that the operating system is properly configured and the CA application software is actively and properly using the C2 security controls, including identification and authentication, discretionary access controls, and audit.

3.6.6 Life Cycle Security Controls

Description: This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of fail-safe design and implementation techniques (e.g., defensive programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) levels IV and V [20], independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM) [19].

Objective: To ensure that the security features are maintained throughout the life cycle.

Security Criticality: The life-cycle security reduces the chances of intentional Trojan horses.

Non-Security Criticality: This component is not otherwise critical.

Examples: An agency has an internal configuration management and life cycle department. The personnel in this department ensure that product updates maintain the expected level of security.

Baseline Recommendation: There are no requirements in this area. These requirements may be overkill for the recommended set of applications.

Compliance Audit Procedure: None

3.6.7 Network Security Controls

Description: This subcomponent addresses network security related controls, including firewalls.

Objective: To describe network security controls.

Security Criticality: The network security controls are critical to the security of the CA to protect against the hacking threat.

Non-Security Criticality: This component is not otherwise critical.

Examples: A CA is protected by a proxy server firewall.

Baseline Recommendation: It is assumed that the CA is either off-line or on the agency enterprise network. If the CA is operated by a third party and networked to public network(s) including the Internet, the CA shall be protected by a firewall that is compliant with the US Firewall protection profile [18]. The CA should be protected in order to protect against the hacking threat from external sources on the Internet.

Compliance Audit Procedure: The auditor shall verify the above connectivity assumption.

3.6.8 Cryptographic Module Engineering Controls

Description: This subcomponent addresses the following aspects of a cryptographic module: identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests. Requirements may be expressed through reference to a standard such as U.S. FIPS 140-1.

Objective: To ensure the cryptographic modules are adequately described in the policy.

Security Criticality: Cryptographic module engineering is critical to the protection of cryptographic operations and the storage of private keys.

Non-Security Criticality: This subcomponent is not otherwise critical.

Examples: The CA cryptographic module complies with the FIPS 140-1 level 2 requirements.

Baseline Recommendation: The CA shall use FIPS 140-1 level 2 validated cryptographic modules. The RAs and end entities shall use FIPS 140-1 level 1 validated cryptographic modules. The RAs shall physically protect their cryptographic modules at all times.

FIPS 140-1 compliance ensures that the private key is protected, and the private key and the cryptographic module may be used only by authorized personnel. Since Level 1 does not require any physical security protection, it is recommended that RAs use procedural means to protect their cryptographic modules.

Compliance Audit Procedure: The auditor shall verify that the CA and RA are using appropriate FIPS 140-1 validated modules. A list of 140-1 validated products is available from http://csrc.nist.gov/cryptval/.

3.7 CERTIFICATE AND CRL PROFILES

This component is used to specify the certificate format and, if CRLs are used, the CRL format. Assuming use of the X.509 certificate and CRL formats, this includes information on profiles, versions, and extensions used.

This component has two subcomponents:

- Certificate Profile
- CRL Profile

This field lists certificate policies, recognized by the issuing CA, that apply to the certificate, together with optional qualifier information pertaining to these certificate policies. Typically, different certificate policies will relate to different applications which may use the certified key (for additional information, see [16]). This field is defined as follows:

3.7.1 Certificate Profile

Description: This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the PKIX Part I profile[17]):

- Version number(s) supported
- Certificate extensions populated and their criticality
- Cryptographic algorithm object identifiers
- Name forms used for the CA, RA, and end entity names
- Name constraints used and the name forms used in the name constraints
- Applicable certificate policy Object Identifier(s)
- Usage of the policy constraints extension
- Policy qualifiers syntax and semantics
- Processing semantics for the critical certificate policy extension

Extensions, when used, must be included in both the CA certificate and end-user certificates.

Objective: To document the certificate extensions used.

Security Criticality: This component is security critical to ensure that the certificate is populated with the proper policy extension.

Non-Security Criticality: The component is critical for interoperability.

Examples: See X.509 Draft Amendment [1].

Baseline Recommendation: The CA shall generate MISPC compliant version 3 certificates:

- **Version number(s) supported:** X.509 version 3
- **Certificate extensions populated and their criticality:** See MISPC
- **Cryptographic algorithm object identifiers:** See MISPC
- **Name forms used for the CA, RA, and end entity names:** DN
- **Name constraints used and the name forms used in the name constraints:** Generally, agency CA shall be constrained to the DIT under the agency DN
- **Applicable certificate policy Object Identifier(s):** The OID for this policy
- **Usage of the policy constraints extension:** No
- **Policy qualifiers syntax and semantics:** None
- **Processing semantics for the critical certificate policy extension:** Not Applicable

Compliance Audit Procedure: The auditor shall take a statistical sample of certificates issued since the last audit and validate that the certificates match the profile.

3.7.2 CRL Profile

Description: A CRL contains fields for a version, signature, issuer name, date issued, issue date for next update, and the revoked certificates. This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the PKIX Part I profile):

- Version numbers supported for CRLs
- CRL and CRL entry extensions populated and their criticality.

Objective: To define the CRL profile.

Security Criticality: This component is not security critical as long as the CRL is X.509 version 2 compliant.

Non-Security Criticality: This subcomponent is critical for interoperability.

Examples: See DAM [1]

Baseline Recommendation: The CA shall generate CRLs that follow the profile in the MISPC [8].

Compliance Audit Procedure: The auditor shall take a statistical sample of CRLs issued since the last audit and validate that the CRLs match the profile.

3.8 SPECIFICATION ADMINISTRATION

This component is used to specify how this particular practices and policy specification will be maintained.

It contains the following subcomponents:

- Specification Change Procedures
- Publication and Notification Procedures
- CPS Approval Procedures

3.8.1 Specification Change Procedures

Description: It will occasionally be necessary to change certificate policies and Certification Practice Statements. Some of these changes will not materially reduce the assurance that a certificate policy or its implementation provides, and will be judged by the policy administrator as not changing the acceptability of certificates asserting the policy for the

purposes for which they have been used. Such changes to certificate policies and Certification Practice Statements need not require a change in the certificate policy Object Identifier or the CPS pointer (URL). Other changes to a specification will change the acceptability of certificates for specific purposes, and these changes will require changes to the certificate policy Object Identifier or CPS pointer (URL).

This subcomponent contains the following information:

- A list of specification components, subcomponents, and/or elements thereof that can be changed without notification and without changes to the certificate policy Object Identifier or CPS pointer (URL).
- A list of specification components, subcomponents, and/or elements thereof that may change following a notification period without changing the certificate policy Object Identifier or CPS pointer (URL). The procedures to be used to notify interested parties (relying parties, certification authorities, etc.) of the certificate policy or CPS changes are described. The description of notification procedures includes the notification mechanism, notification period for comments, mechanism to receive, review and incorporate the comments, mechanism for final changes to the policy, and the period before final changes become effective.
- A list of specification components, subcomponents, and/or elements, changes to which require a change in certificate policy Object Identifier or CPS pointer (URL).

Objective: To define which portions of a CP or CPS may be changed, and what notice will be given to users of those changes.

Security Criticality: The relying parties must be kept informed of policy changes.

Non-Security Criticality: This subcomponent is critical in that users must know if they can accept a CP as providing a fixed level of assurance, or must review changes to the policy that will affect security.

Examples:. The contact name can change without notification.

Baseline Recommendation: No components of this policy shall change without proper notification. Any or all components may be changed without changing the policy object identifier.

Compliance Audit Procedure: The auditor shall determine if the policy changed since the last compliance audit. If yes, the auditor shall verify that the change notifications were in accordance with the notification procedures described in this policy.

3.8.2 Publication and Notification Procedures

Description: This subcomponent contains the following elements:

- A list of components, subcomponents, and elements thereof that exist but that are not made publicly available
- Descriptions of mechanisms used to distribute the certificate policy definition or CPS, including access controls on such distribution.

Objective: To provide a means for the subscribers and relying parties to obtain the policy and the CPS.

Security Criticality: This subcomponent allows the interested parties obtain the policy.

Non-Security Criticality: This subcomponent is not otherwise critical.

Examples: A CA uses a public repository to distribute certificate policy.

Baseline Recommendation: The agency shall make the CP and the CPS available in electronic form under a URL and under the CA DN with a newly defined X.500 directory attribute – certificatePolicy. The CP and CPS shall be digitally signed by the CA. All information in the CP and CPS shall be available publicly.

Compliance Audit Procedure: The auditor shall verify that the latest CP and CPS are stored under the agency URL and CA DN.

3.8.3 CPS Approval Procedures

Description: In a certificate policy definition, this subcomponent describes how the compliance of a specific CPS with the certificate policy can be determined.

Objective: To allow the CP to establish a uniform method for demonstrating compliance.

Security Criticality: This subcomponent is not security critical.

Non-Security Criticality: This subcomponent may be critical with respect to legal or contractual concerns..

Examples: The CPS shall be accredited as satisfying the requirements of the specified CP by TBD (auditor or accreditation authority).

Baseline Recommendation: This subcomponent is beyond the scope of this document.

Compliance Audit Procedure: The auditor will verify that the review of the CPS being conducted meets the CP's requirements.

4 REFERENCES

1. ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology – Open Systems Interconnection: The Directory: Authentication Framework," June 1997.
2. Privacy Enhancement for Internet Electronic Mail, S. Kent, Part II: Certificate- Based Key Management," Internet RFC 1422, 1993.
3. American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce, Draft 1995.
4. Michael. S. Baum, Federal Certification Authority Liability and Policy, NIST-GCR- 94-654, June 1994.
5. Certificate Policy and Certification Practices Framework, S. Chokhani and W. Ford, Informational RFC, IETF PKIX Part IV, July 1997.
6. Pubic Key Infrastructure Technical Specification: Part A – Technical Security Policy, Noel A. Nazario, NIST. (Available from http://csrc/nist.gov/pki)
7. General Procedures for Registering Computer Security Objects, NIST IR 5308, December, 1993. (Up to date information at http://csrc.nist.gov/csor)
8. Minimum Interoperability Specification for PKI Components, NIST Special Publication 800-15 Version 1, January 1998. (Available from http://csrc/nist.gov/pki)
9. Computer Security Policy, Computer Security Laboratory (CSL) Bulletin CSL94-01, NIST, January, 1994.
10. People: An Important Asset in Computer Security, CSL Bulletin CSL93-10, NIST, October, 1993.
11. Security Requirements for Cryptographic Modules, NIST, FIPS PUB 140-1, January 1994.
12. Automated Password Generator, Federal Information Processing Standard 181, October, 1993.
13. Minimum Security Requirements for Multi-User Operating Systems, CSL, NISTIR 5153, NIST, March, 1993.
14. Guidance on the Selection of Low Level Assurance Evaluated Products, CSL Bulletin, CSL96-04, NIST, April, 1996.
15. Guideline for Automatic Data Processing Risk Analysis, National Bureau of Standards.
16. Pubic Key Infrastructure Technical Specification: Part C - Concept of Operations, William E. Burr, National Institute of Standards and Technology (NIST).

17. R. Housley, W. Ford, W. Polk, D. Solo, Internet Public Key Infrastructure, X.509 Certificate and CRL Profile, draft-ietf-pkix-ipki-part1-07.txt, March 25,1998
18. US Government Traffic Filter Firewall Protection Profile for Low Risk Environments, Version 1.0, NIST, December 1997, http://csrc.nist.gov/nistpubs/cc/pp/pplist.htm#FIREWALL.
19. Marc. Paulk, Bill Curtis, Mary Beth Chrissis, and Charles V. Weber, “Capability Maturity Model, Version 1.1,” IEEE Software, Vol. 10, No. 4, July 1993, pp. 18-27.
20. Trusted Software Development methodology, SDI-S-SD-91-000007, June 17, 1992.
21. Trusted Computer System Evaluation Criteria, DOD-STD-5200.28, December 1985.

5 LIST OF ACRONYMS

ABA	American Bar Association
ANSI	American National Standards Institute
ASN	Abstract Syntax Notation
CA	Certification Authority
CMM	Capability Maturity Model
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DAM	Draft Amendment
DES	Data Encryption Standard
DH	Diffie-Hellman
DN	Distinguished Name
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standard
I&A	Identification and Authentication
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IG	Inspector General
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunications Union
MISPC	Minimum Interoperability Specification for PKI Components
NIST	National Institute of Standards and Technology
OID	Object Identifier
PIN	Personal Identification Number
PKI	Pubic Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)

RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, and Adleman
SHA-1	Secure Hash Algorithm - Revision 1
TDSM	Trusted Software Development Methodology
URL	Uniform Resource Locator
US	United States

APPENDIX A: GENERAL PROVISIONS

This appendix contains preliminary suggestions for addressing issues from the General Provisions component of the Certificate Policy and Certification Practice Statement Framework. The issues addressed are outside the scope of a Security Recommendation document. This material is provided here as an introduction to the issues and possible ways to approach them. The statements made should not be used in certificate policies or Certification Practice Statements without been reviewed by legal counsel. The General Provisions component contains the following subcomponents:

1. Liability
2. Obligations
3. Financial Responsibility
4. Interpretation and Enforcement
5. Fee
6. Publication and Repositories
7. Compliance Audit
8. Confidentiality
9. Intellectual Property Rights

Each subcomponent may need to separately state provisions applying to the entity types: CA, repository, RA, subscriber, and relying party. (Specific provisions regarding subscribers and relying parties are only applicable in the Liability and Obligations subcomponents.)

The agency General Counsel should be consulted in formulating the certificate policy and CPS for this component. The following are some preliminary suggestions.

A.1 LIABILITY

Description: This subcomponent contains, for each entity type, any applicable provisions regarding apportionment of liability, such as the following elements:

1. Warranties and limitations on warranties
2. Types of damages covered (e.g., indirect, special, consequential, incidental, punitive, liquidated damages, negligence and fraud) and disclaimers
3. Loss limitations (caps) per certificate or per transaction
4. Other exclusions (e.g., Acts of God, other party responsibilities)

Objective: This subcomponent is used to define types of liability and limitation on liabilities for the various losses.

Security Criticality: This subcomponent is not security critical.

Non-Security Criticality: This subcomponent is critical in the sense that it tells the relying parties who is responsible financially, to what extent, and under what circumstances.

Examples: This is a legal issue and examples are beyond the scope of the Baseline Security Recommendation.

Baseline Recommendation: The baseline policy should either state “no stipulation” for this subcomponent or ask the agency General Counsel if a liability statement is required and what it should be.

Compliance Audit Procedure: The auditor shall verify that the CA is able to meet its obligations and potential liabilities.

A.2 OBLIGATIONS

Description: This subcomponent contains, for each entity type, any applicable provisions regarding the entity's obligations to other entities. Such provisions may include the following elements as applicable.

CA or a RA obligations may include:

1. Notifying subscribers of the issuance of their certificates.
2. Notifying entities, other than the subject of the certificate, of the issuance of a certificate.
3. Notifying subscribers of the revocation or suspension of their certificates.
4. Notifying entities, other than the subject of the certificate, of the revocation or suspension of a certificate.
5. Posting newly issued certificates in repositories or databases
6. Generating CRLs or recording revocations in repositories or databases

Subscriber obligations may include:

1. Making accurate representations in certificate applications
2. Protecting its private key.
3. Observing restrictions on private key and certificate use.

4. Notifying the CA or RA upon private key compromise

Rrelying party obligations may include:

1. Using certificates only for the purposes for which they were issued.
2. Validating all digital signatures
3. Checking certificates for revocation and suspension
4. Acknowledging applicable liability caps and warranties

A repository may have the obligation to publish certificates and revocation information in a timely manner.

Objective: This subcomponent establishes the duties and responsibilities of certificate management service providers and users.

Security Criticality: It is important that the subscribers and/or RAs request timely revocation of certificates. It is important that the CA revoke certificates in a timely manner.

Non-Security Criticality: To properly use certificates, the CA, repository, or subscriber must provide certificates and CRLs to relying parties in a timely fashion.

Examples: The examples are self-evident.

Baseline Recommendation: A CA shall notify the subscriber of the revocation or suspension of her certificate. The notification mechanism shall be a digitally signed electronic mail message from the CA. A CA shall send the subscriber certificates to a repository immediately upon issuance. A CA shall send Certificate Revocation Lists (CRLs) to a repository immediately upon issuance.

A subscriber shall provide accurate identification and authentication information during the initial registration and any subsequent interactions with the CA or the RA including rekeying and revocation requests. A subscriber shall protect her private key as described in the key management section. A subscriber shall immediately notify the RA in the case of private key compromise or loss of the private key token.

A relying party shall obtain the most current periodic CRL and check the certificates against it. If a certificate is in the CRL, the relying party may not use the certificate securely and reliably.

A repository shall publish certificates and CRLs immediately upon receipt from the CA.

Compliance Audit Procedure: The auditor shall check the appropriate audit logs of the CA to ensure that a statistical sample of certificates and CRLs are sent to the repository immediately after issuance.

A repository audit logs shall be checked to ensure that a statistical sample of certificates and CRLs are posted immediately after receipt from the CA.

A.3 FINANCIAL RESPONSIBILITY

Description: This subcomponent contains any applicable provisions regarding financial responsibilities for CAs, repositories, and RAs, such as:

1. Indemnification of CA and/or RA by relying parties
2. Fiduciary relationships (or lack thereof) between the various entities
3. Administrative processes (e.g., accounting, audit, etc.)

Objective: The purpose of this subcomponent is to indemnify the CA and RA

Security Criticality: This element is not security critical.

Non-Security Criticality: This element may limit the financial risk for the CA and RA

Examples: Since this is a legal issue, it is beyond the scope of the effort.

Baseline Recommendation: This component should be developed with the assistance from the agency General Counsel.

Compliance Audit Procedure: None

A.4 INTERPRETATION AND ENFORCEMENT

Description: This subcomponent contains any applicable provisions regarding interpretation and enforcement of the certificate policy or CPS, addressing such topics as:

1. Governing law
2. Survivability provisions, survival, merger, and notice
3. Dispute resolution procedures

Objective: The purpose of this subcomponent is to provide legal foundation for enforcement of the legal, liability, and fiduciary stipulations in the CP or CPS.

Security Criticality: This subcomponent is not security critical.

Non-Security Criticality: This subcomponent is critical in terms ensuring legal enforceability of all or parts of the CP and CPS.

Examples: Since this is a legal issue, examples are beyond the scope of this document.

Baseline Recommendation: The agency General Counsel should be consulted in drafting this subcomponent.

Compliance Audit Procedure: None.

A.5 FEES

Description: This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs, such as:

1. Certificate issuance or renewal fees
2. Certificate access fee
3. Revocation or status information access fee
4. Fees for other services such as policy information
5. Refund policy

Objective: The purpose of this subcomponent is to establish who is paying for the various certificate-related services.

Security Criticality: This component is not security critical.

Non-Security Criticality: This component is not critical otherwise.

Examples: The subscriber shall pay $25 for the initial certificate and $10 for each electronic renewal. The relying party shall pay $0.30 for each certificate access and $3.00 for each CRL access.

Baseline Recommendation: Each agency should make its own determination.

Compliance Audit Procedure: If there are fees, the auditor shall examine the accounts of the CA, RA, and repository for accuracy of charges.

A.6 PUBLICATION AND REPOSITORIES

Description: This subcomponent contains any applicable provisions regarding:

1. A CA's obligations to publish information regarding its practices, its certificates, and the current status of such certificates
2. Publication frequency
3. Access control on published information objects including certificate policy definitions, CPS, certificates, certificate status, and CRLs
4. Requirements pertaining to the use of repositories operated by CAs or by other independent parties

Objective: The objective of this subcomponent is to describe the publication and access requirements for the CP/CPS, certificates, and CRLs.

Security Criticality: The timely issuance of CRLs is security critical.

Non-Security Criticality: The timely publication of certificates and CRLs is required for the relying parties to use these objects.

Examples: The examples are self-evident.

Baseline Recommendation: See section on Obligations. There shall be no access control on reading the certificate policy definitions, CPS, certificates, certificate status, and CRL information.[4]

Compliance Audit Procedure: None

A.7 COMPLIANCE AUDIT

Description: This subcomponent addresses the following:

[4] It is envisioned that the information such as the certificate policy, CPS, certificates, and CRL are public and are available to the relying parties at no cost. Thus, this information can be viewed by anyone.

1. Frequency of compliance audit for each entity
2. Identity of the auditor
3. Auditor's relationship to the entity being audited
4. List of topics covered under the compliance audit
5. Actions taken as a result of a deficiency found during compliance audit
6. Compliance audit results: who are they shared with (e.g., subject CA, RA, and/or end entities), who provides them (e.g., entity being audited or auditor), and how they are communicated

Objective: The purpose of this subcomponent is to provide an independent proof of CA and other components' compliance with this CP/CPS.

Security Criticality: This element is security critical to ensure that the security controls are properly enforced.

Non-Security Criticality: This element is otherwise critical to ensure that CA and other components operate correctly.

Examples: The examples are self-evident.

Baseline Recommendation: The audit shall be conducted 3 months after the establishment of the CA and every 24 months thereafter. The auditor shall be from the agency Inspector General (IG) office and shall be appointed by the IG. The topics covered are all the topics identified in this policy. If the auditor finds a minor deficiency, the auditor shall notify the appropriate entity (CA, RA, repository, or subscriber). If the deficiency is major, the auditor shall give appropriate time for fixing the deficiency and perform an audit of the failed element(s). If the entity (including the CA) has not corrected the action, its certificate shall be revoked.

The compliance audit results shall be published in a repository.

Compliance Audit Procedure: Not applicable.

A.8 CONFIDENTIALITY POLICY

Description: This subcomponent addresses the following:

1. Types of information that must be kept confidential[5] by CA or RA
2. Types of information not considered confidential
3. Who is entitled to be informed of reasons for revocation and suspension of certificates
4. Policy on release of information to law enforcement officials
5. Information that can be revealed as part of civil discovery
6. Conditions upon which CA or RA may disclose (e.g., upon owner's request)
7. Any other circumstances under which confidential information may be disclosed

Objective: The objective of this subcomponent is to inform the subscriber which information is considered confidential, but may have to be released under specified circumstances. Clarifying this avoids future dispute and legal action by the subscribers.

Security Criticality: This element is not security critical.

Non-Security Criticality: This element is legally critical.

Examples: Types of confidential information are the documents (e.g., driver's license) used to identify and authenticate the subscriber.

Baseline Recommendation: Most information, including revocation reasons are not considered confidential.[6] The only information that may be confidential is parts of documents provided during identification and authentication (I&A). The agency General Counsel will determine which information from the I&A shall be confidential. The CA and RA shall maintain detailed technical and/or non-technical procedures to maintain the confidentiality of this information. The CPS shall describe these controls. For the CPS, it is recommended that the means include the physical security of the computers containing the information, network security protection (i.e., firewalls) if a computer containing the information is connected to public networks, and C2 level discretionary access controls.

The confidential information may be released upon subscriber request, criminal investigation, and civil or criminal court proceeding in accordance with the agency regulations. The agency General Counsel shall be consulted to further develop the policy and procedures. These procedures shall be described in the CPS.

---

[5] The term "confidential" here does not represent one of the hierarchical classifications used by the various security policies including, law enforcement and national security.

[6] The revocation reasons are not considered confidential. Those who are sensitive to their marital status change being determined from revocations, should use maiden names.

Compliance Audit Procedure: The auditor shall examine the protection mechanisms used to protect the confidentiality of the information. The auditor shall examine all the disclosure of information since the last audit to verify that the defined policy and procedures were followed.

A.9 INTELLECTUAL PROPERTY RIGHTS

Description: This subcomponent addresses ownership rights of certificates, practice/policy specifications, names, and keys.

Objective: This subcomponent protects any intellectual property claims.

Security Criticality: This subcomponent is not security critical.

Non-Security Criticality: The criticality is dependent on the person or company requirements.

Examples: A company has pre-patent information that is considered the company's intellectual property.

Baseline Recommendation: No stipulation.

Compliance Audit Procedure: Not applicable.